

Facebook and the GFW of China

Geoff Huston, Byron Ellacott
APNIC

Outside

```
$ dig +short www.facebook.com
star.c10r.facebook.com.
69.171.229.25
$ dig +short AAAA www.facebook.com
star.c10r.facebook.com.
2a03:2880:10:6f08:face:b00c:0:1
```

Deep Inside China

```
$ dig +short www.facebook.com
1.1.1.1
$ dig +short AAAA www.facebook.com
2001:da8:112::21ae
```

Outside

```
$ dig +short www.facebook.com
star.c10r.facebook.com.
69.171.229.25
$ dig +short AAAA www.facebook.com
star.c10r.facebook.com.
2a03:2880:10:6f08:face:b00c:0:1
```

Deep Inside China

```
$ dig +short www.facebook.com
1.1.1.1
$ dig +short AAAA www.facebook.com
2001:da8:112::21ae
```

Outside

```
$ whois 69.171.229.25
```

```
NetRange:      69.171.224.0 - 69.171.255.255
CIDR:          69.171.224.0/19
OriginAS:      AS32934
NetName:       TFBNET3
NetHandle:     NET-69-171-224-0-1
Parent:        NET-69-0-0-0-0
NetType:       Direct Assignment
RegDate:       2010-08-05
Updated:       2012-02-24
Ref:           http://whois.arin.net/rest/net/
NET-69-171-224-0-1

OrgName:       Facebook, Inc.
OrgId:         THEFA-3
Address:       1601 Willow Rd.
City:          Menlo Park
StateProv:    CA
PostalCode:   94025
Country:      US
RegDate:      2004-08-11
Updated:      2012-04-17
Ref:          http://whois.arin.net/rest/org/THEFA-3

OrgTechHandle: OPERA82-ARIN
OrgTechName:   Operations
OrgTechPhone:  +1-650-543-4800
OrgTechEmail:  noc@fb.com
OrgTechRef:    http://whois.arin.net/rest/poc/OPERA82-ARIN

OrgAbuseHandle: OPERA82-ARIN
OrgAbuseName:  Operations
OrgAbusePhone: +1-650-543-4800
OrgAbuseEmail: noc@fb.com
OrgAbuseRef:   http://whois.arin.net/rest/poc/OPERA82-ARIN
```

Deep Inside China

```
$ whois 1.1.1.1
```

```
inetnum:       1.1.1.0 - 1.1.1.255
netname:       Debogon-prefix
descr:         APNIC Debogon Project
descr:         APNIC Pty Ltd
country:       AU
admin-c:       AR302-AP
tech-c:        AR302-AP
mnt-by:        APNIC-HM
mnt-routes:    MAINT-AU-APNIC-GM85-AP
mnt-irt:       IRT-APNICRANDNET-AU
status:        ASSIGNED PORTABLE
changed:       hm-changed@apnic.net 20110922
source:        APNIC

irt:           IRT-APNICRANDNET-AU
address:       PO Box 3646
address:       South Brisbane, QLD 4101
address:       Australia
e-mail:        abuse@apnic.net
abuse-mailbox: abuse@apnic.net
admin-c:       AR302-AP
tech-c:        AR302-AP
mnt-by:        MAINT-AU-APNIC-GM85-AP
changed:       hm-changed@apnic.net 20110922
source:        APNIC

role:          APNIC RESEARCH
```

Outside

```
$ whois 69.171.229.25
```

```
NetRange: 69.171.224.0 - 69.171.255.255
CIDR: 69.171.224.0/19
OriginAS: AS32934
NetName: TFBNET3
NetHandle: NET-69-171-224-0-1
Parent: NET-69-0-0-0-0
NetName:
Registrar:
Updated:
Ref:
Facebook, INC
http://whois.arin.net/rest/net/
NET-69-171-224-0-1
```

```
OrgName: Facebook, Inc.
OrgId: THEFA-3
Address: 1601 Willow Rd.
City: Menlo Park
StateProv: CA
PostalCode: 94025
Country: US
RegDate: 2004-08-11
Updated: 2012-04-17
Ref: http://whois.arin.net/rest/org/THEFA-3
```

```
OrgTechHandle: OPERA82-ARIN
OrgTechName: Operations
OrgTechPhone: +1-650-543-4800
OrgTechEmail: noc@fb.com
OrgTechRef: http://whois.arin.net/rest/poc/OPERA82-ARIN
```

```
OrgAbuseHandle: OPERA82-ARIN
OrgAbuseName: Operations
OrgAbusePhone: +1-650-543-4800
OrgAbuseEmail: noc@fb.com
OrgAbuseRef: http://whois.arin.net/rest/poc/OPERA82-ARIN
```

Deep Inside China

```
$ whois 1.1.1.1
```

```
inetnum: 1.1.1.0 - 1.1.1.255
netname: Deboqon-prefix
descr: APNIC Deboqon Project
descr: APNIC Pty Ltd
country: AU
admin-c: AR302-AP
tech-c: AR302-AP
mn:
mn:
mn: APNIC Labs! -AP
st:
changed: hm-changed@apnic.net 20110922
source: APNIC

irt: IRT-APNICRANDNET-AU
address: PO Box 3646
address: South Brisbane, QLD 4101
address: Australia
e-mail: abuse@apnic.net
abuse-mailbox: abuse@apnic.net
admin-c: AR302-AP
tech-c: AR302-AP
mnt-by: MAINT-AU-APNIC-GM85-AP
changed: hm-changed@apnic.net 20110922
source: APNIC

role: APNIC RESEARCH
```

~~Outside~~

Inside

So let's focus on that inside address:
1.1.1.1

~~Outside~~

Inside

So let's focus on that inside address:
1.1.1.1

is this the "real thing" or just a local route to some local black hole?

~~Outside~~

Inside

So let's focus on that inside address:
1.1.1.1

is this the "real thing" or just a local route to some local black hole?

Let's resume the inside/Outside examination, but focus just on the address 1.1.1.1

Outside

```
$ traceroute 1.1.1.1
traceroute to 1.1.1.1 (1.1.1.1), 64 hops max, 52 byte packets
 1 202.158.221.221 (202.158.221.221) 0.266 ms 0.202 ms
0.194 ms
 2 ge-4-0-0.bb1.b.cbr.aarnet.net.au (202.158.208.81) 0.491 ms
0.438 ms 0.424 ms
 3 so-0-1-0.bb1.b.mel.aarnet.net.au (202.158.194.42) 8.001 ms
8.000 ms 7.992 ms
 4 xe-0-0-0.pe1.a.mel.aarnet.net.au (202.158.200.12) 8.110 ms
8.088 ms 8.078 ms
 5 gw1.xe-0-0-2.pe1.a.mel.aarnet.net.au (202.158.210.41)
12.165 ms 12.193 ms 12.159 ms
 6 66.249.95.232 (66.249.95.232) 12.823 ms 13.254 ms
66.249.95.234 (66.249.95.234) 20.282 ms
 7 209.85.249.52 (209.85.249.52) 134.637 ms 109.393 ms
109.426 ms
 8 64.233.175.3 (64.233.175.3) 128.052 ms 113.782 ms
64.233.175.1 (64.233.175.1) 113.192 ms
 9 209.85.255.34 (209.85.255.34) 114.562 ms
209.85.255.36 (209.85.255.36) 118.550 ms 133.640 ms
10 64.233.174.178 (64.233.174.178) 211.021 ms 211.275 ms
211.694 ms
11 72.14.239.82 (72.14.239.82) 263.661 ms 287.038 ms
264.518 ms
12 216.239.48.41 (216.239.48.41) 269.732 ms
72.14.239.65 (72.14.239.65) 270.545 ms
216.239.48.41 (216.239.48.41) 270.244 ms
13 72.14.235.11 (72.14.235.11) 279.278 ms 277.787 ms
66.249.95.230 (66.249.95.230) 277.315 ms
14 72.14.236.99 (72.14.236.99) 415.698 ms
72.14.236.147 (72.14.236.147) 278.543 ms
72.14.236.99 (72.14.236.99) 412.531 ms
15 209.85.252.47 (209.85.252.47) 256.836 ms
209.85.252.81 (209.85.252.81) 253.370 ms
209.85.252.47 (209.85.252.47) 254.984 ms
16 65.210.126.78 (65.210.126.78) 255.713 ms 253.913 ms
253.865 ms
```

Inside

```
$ traceroute 1.1.1.1
traceroute to 1.1.1.1 (1.1.1.1), 64 hops max, 52 byte packets
 1 254 (220.247.145.254) 6.620 ms 1.774 ms 2.561 ms
 2 * * *
 3 192.168.9.5 (192.168.9.5) 6.718 ms 3.322 ms 5.324 ms
 4 159.226.253.189 (159.226.253.189) 25.557 ms 26.145 ms
27.191 ms
 5 8.130 (159.226.253.57) 26.059 ms 27.225 ms 25.889 ms
 6 8.198 (159.226.253.50) 27.060 ms 29.788 ms 29.476 ms
 7 8.192 (159.226.254.254) 64.767 ms 66.801 ms 66.768 ms
 8 72.14.221.138 (72.14.221.138) 100.753 ms 105.117 ms
99.613 ms
 9 209.85.241.56 (209.85.241.56) 101.914 ms
209.85.241.58 (209.85.241.58) 105.561 ms 101.748 ms
10 66.249.94.31 (66.249.94.31) 175.902 ms
66.249.94.123 (66.249.94.123) 149.653 ms
66.249.94.31 (66.249.94.31) 149.498 ms
11 64.233.175.3 (64.233.175.3) 150.364 ms
64.233.175.1 (64.233.175.1) 150.610 ms 147.552 ms
12 209.85.255.36 (209.85.255.36) 163.323 ms *
209.85.255.58 (209.85.255.58) 154.349 ms
13 64.233.174.178 (64.233.174.178) 353.593 ms 286.374 ms
312.122 ms
14 72.14.239.80 (72.14.239.80) 245.300 ms
72.14.239.82 (72.14.239.82) 325.655 ms 284.123 ms
15 216.239.48.41 (216.239.48.41) 279.139 ms 274.913 ms
276.807 ms
16 66.249.95.230 (66.249.95.230) 274.683 ms 274.613 ms
66.249.95.228 (66.249.95.228) 273.204 ms
17 72.14.236.147 (72.14.236.147) 313.601 ms
72.14.236.149 (72.14.236.149) 261.617 ms 305.524 ms
18 209.85.252.47 (209.85.252.47) 306.003 ms
209.85.252.81 (209.85.252.81) 276.541 ms 363.910 ms
19 65.210.126.78 (65.210.126.78) 398.681 ms 361.306 ms
366.265 ms
```

Outside

```
$ traceroute 1.1.1.1
traceroute to 1.1.1.1 (1.1.1.1), 64 hops max, 52 byte packets
 1 202.158.221.221 (202.158.221.221) 0.266 ms 0.202 ms
0.194 ms
 2 ge-4-0-0.bb1.b.cbr.aarnet.net.au (202.158.208.81) 0.491 ms
0.438 ms 0.424 ms
 3 so-0-1-0.bb1.b.mel.aarnet.net.au (202.158.194.42) 8.001 ms
8.000 ms 7.992 ms
 4 xe-0-0-0.pe1.a.mel.aarnet.net.au (202.158.200.12) 8.110 ms
8.088 ms 8.078 ms
 5 gw1.xe-0-0-2.pe1.a.mel.aarnet.net.au (202.158.210.41)
12.165 ms 12.193 ms 12.159 ms
 6 66.249.95.232 (66.249.95.232) 12.823 ms 13.254 ms
66.249.95.234 (66.249.95.234) 20.282 ms
 7 209.85.249.52 (209.85.249.52) 134.637 ms 109.393 ms
109.426 ms
 8 64.233.174.178 (64.233.174.178) 353.593 ms 286.374 ms
312.122 ms
 9 209.85.252.81 (209.85.252.81) 253.370 ms
209.85.252.83 (209.85.252.83) 254.984 ms
209.85.252.47 (209.85.252.47) 254.984 ms
10 65.210.126.78 (65.210.126.78) 255.713 ms 253.913 ms
253.865 ms
```

Hang on... BOTH inside and outside ROUTE the packets addressed to 1.1.1.1 to the same endpoint: **65.210.126.78**

Inside

```
$ traceroute 1.1.1.1
traceroute to 1.1.1.1 (1.1.1.1), 64 hops max, 52 byte packets
 1 254 (220.247.145.254) 6.620 ms 1.774 ms 2.561 ms
 2 * * *
 3 192.168.9.5 (192.168.9.5) 6.718 ms 3.322 ms 5.324 ms
 4 159.226.253.189 (159.226.253.189) 25.557 ms 26.145 ms
27.191 ms
 5 8.130 (159.226.253.57) 26.059 ms 27.225 ms 25.889 ms
 6 8.198 (159.226.253.50) 27.060 ms 29.788 ms 29.476 ms
 7 8.192 (159.226.254.254) 64.767 ms 66.801 ms 66.768 ms
 8 72.14.221.138 (72.14.221.138) 100.753 ms 105.117 ms
99.613 ms
 9 209.85.241.56 (209.85.241.56) 101.914 ms
209.85.241.58 (209.85.241.58) 105.561 ms 101.748 ms
10 66.249.94.31 (66.249.94.31) 175.902 ms
209.85.255.58 (209.85.255.58) 154.349 ms
11 64.233.174.178 (64.233.174.178) 353.593 ms 286.374 ms
312.122 ms
12 72.14.239.80 (72.14.239.80) 245.300 ms
72.14.239.82 (72.14.239.82) 325.655 ms 284.123 ms
13 216.239.48.41 (216.239.48.41) 279.139 ms 274.913 ms
276.807 ms
14 66.249.95.230 (66.249.95.230) 274.683 ms 274.613 ms
66.249.95.228 (66.249.95.228) 273.204 ms
15 72.14.236.147 (72.14.236.147) 313.501 ms
72.14.236.149 (72.14.236.149) 261.617 ms 305.524 ms
16 209.85.252.47 (209.85.252.47) 306.003 ms
209.85.252.81 (209.85.252.81) 276.541 ms 363.910 ms
17 65.210.126.78 (65.210.126.78) 398.681 ms 361.306 ms
366.265 ms
```

But 65.210.126.78 is Google!

```
$ whois 65.210.126.78
```

```
#
```

```
# ARIN WHOIS data and services are subject to the Terms of Use  
# available at: https://www.arin.net/whois\_tou.html
```

```
#
```

```
#
```

```
# The following results may also be obtained via:  
# http://whois.arin.net/rest/nets;q=65.210.126.78?  
showDetails=true&showARIN=false&ext=netref2
```

```
#
```

```
MCI Communications Services, Inc. d/b/a Verizon Business UUNET65  
(NET-65-192-0-0-1) 65.192.0.0 - 65.223.255.255
```

```
GOOGLE INC UU-65-210-126-72 (NET-65-210-126-72-1) 65.210.126.72 -  
65.210.126.79
```

So...

Why is 1.1.1.1 being routed into Google?



Asia Pacific Network Information Centre
APNIC Pty Ltd
ABN: 42 081 528 010
6 Cordelia Street
PO Box 3646
South Brisbane
QLD 4101 AUSTRALIA

URL www.apnic.net
Enquiries helpdesk@apnic.net
Accounts billing@apnic.net
Phone +61 7 3858 3100
Fax + 61 7 3858 3199

Letter of Authority

2 May 2013

APNIC and Google Joint Research Activity in Dark Traffic Profile

To whom it may concern,

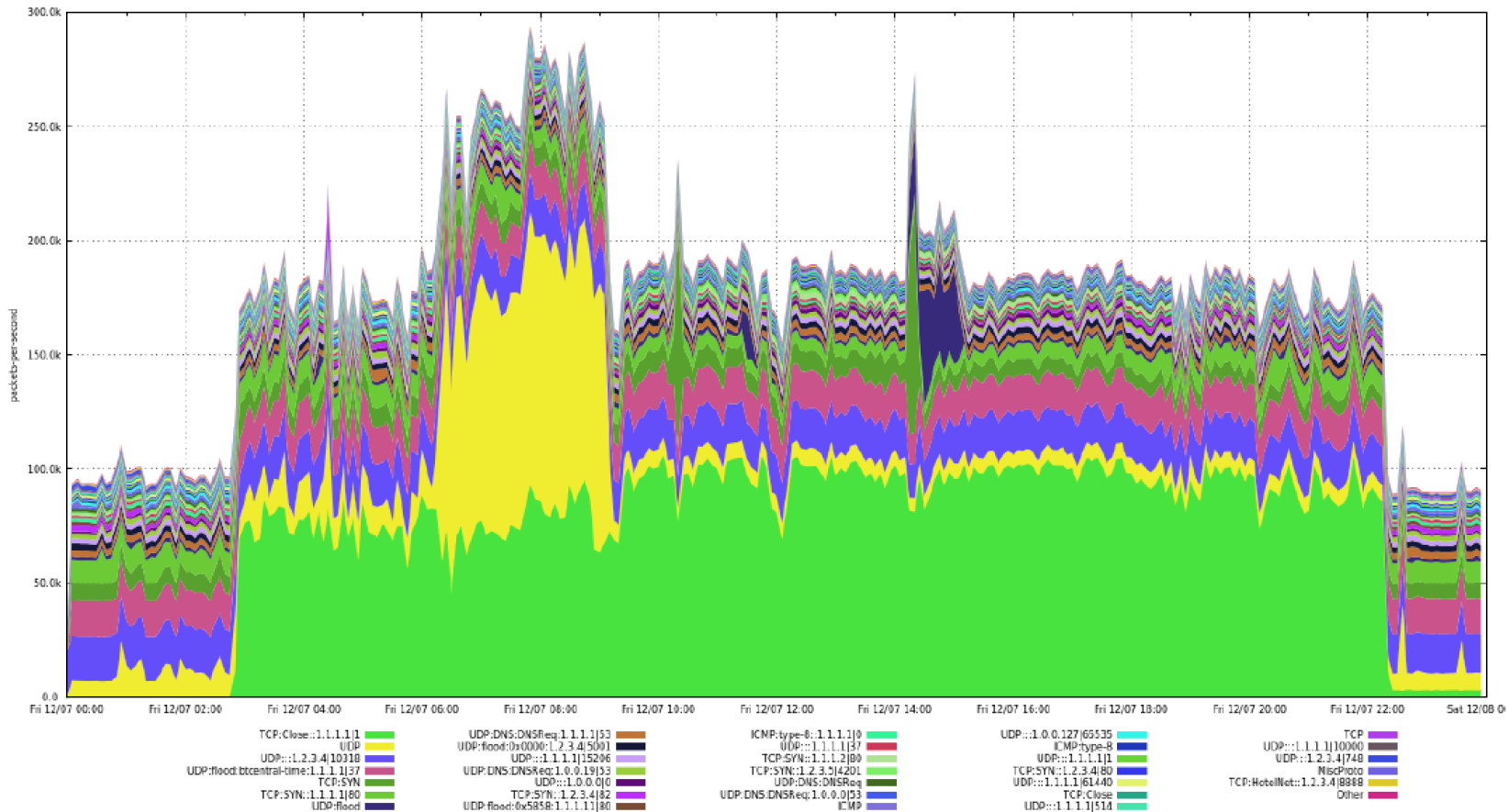
APNIC and Google are cooperating in a project to investigate the properties of unwanted traffic that is being sent to specific destinations in the APNIC-held prefixes 1.0.0.0/24, 1.1.1.0/24 and 1.2.3.0/24. Accordingly, APNIC authorizes Google to periodically advertise a route for these prefixes from AS 15169, and requests that Google's routing peers accept this as a legitimate routing advertisement. This authority is valid for a period of 12 months, until 2 May 2014.

Geoff Huston
Chief Scientist

And there's a darknet traffic collector
at that address!

And there's a darknet traffic collector at that address!

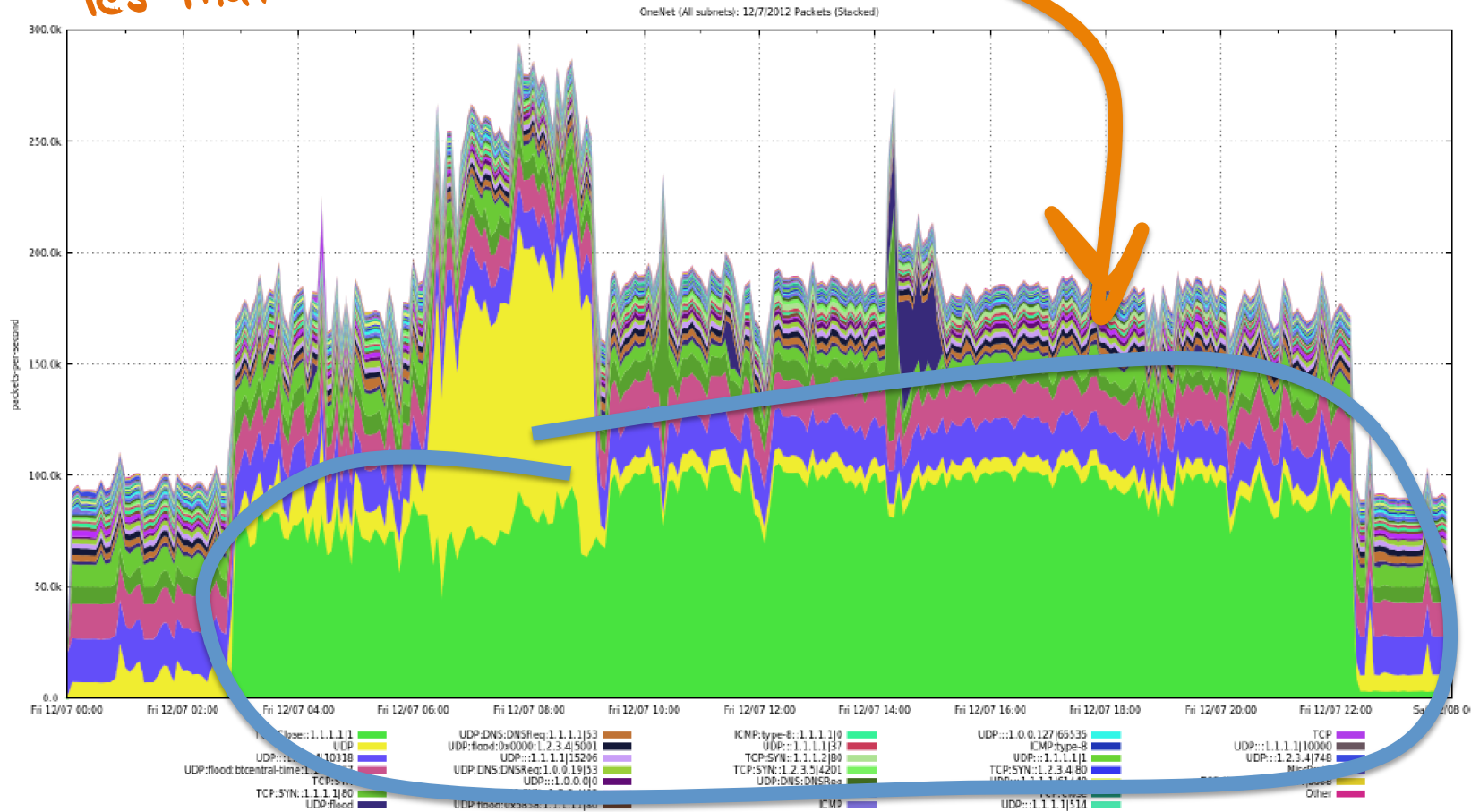
OneNet (All subnets): 12/7/2012 Packets (Stacked)



And here's a small snapshot of what it sees

And there's a darknet traffic collector at that address!

Yes that's incoming TCP SYN to 1.1.1.1 port 80!





Spy Vs. Spy

So, for Facebook in China, exactly who is watching who here?

But at other times it's even stranger...

```
$ dig @m.root-servers.net www.facebook.com
; <<>> DiG 9.9.3-P1 <<>> @m.root-servers.net.    www.facebook.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3195
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.facebook.com    IN    A

;; ANSWER SECTION:
www.facebook.com.    300 IN    A    255.255.255.255

;; Query time: 38 msec
;; SERVER: 2001:dc3::35#53(2001:dc3::35)
;; WHEN: Tue Aug 27 19:07:12 EST 2013
;; MSG SIZE    rcvd: 50
```

But at other times it's even stranger...

```
$ dig @m.root-servers.net www.facebook.com
; <<>> DiG 9.9.3-P1 <<>> @m.root-servers.net. www.facebook.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3195
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.facebook.com IN A

;; ANSWER SECTION:
www.facebook.com. 300 IN A 255.255.255.255

;; Query time: 38 msec
;; SERVER: 2001:dc3::35#53(2001:dc3::35)
;; WHEN: Tue Aug 27 19:07:12 EST 2013
;; MSG SIZE rcvd: 50
```

*Really!
The broadcast address!*

Thanks!